# สรุปความคิดเห็นและข้อสังเกตต่อแนวทางการจัดทำร่างหลักเกณฑ์การตรวจประเมินประจำปี

| ร่างหลักเกณฑ์ฉบับร่างรับฟังความคิดเห็น | ความคิดเห็น/ข้อเสนอแนะ |
|---|---|
| **ส่วนที่ 1 การตรวจประเมินประจำปี** | |
| ข้อ 1 ผู้รับใบอนุญาตต้องจัดให้มีการตรวจประเมินระบบการให้บริการอย่างน้อยปีละหนึ่งครั้ง ให้ครอบคลุมหัวข้ออย่างน้อยดังนี้<br>1.1 การปฏิบัติตามหลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ หมวด 1 ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ หมวด 2 การรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และหมวด 3 การบริหารและการจัดการความเสี่ยงของระบบการให้บริการ<br>1.2 การปฏิบัติตามหลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ<br>1.3 การปฏิบัติตามหลักเกณฑ์การตามลักษณะของการให้บริการ<br>1.4 หัวข้ออื่น ๆ ตามได้รับแจ้งจากสำนักงาน | ● ควรตรวจประเมินปีเว้นปี เนื่องจากเป็นภาระของผู้รับใบอนุญาตในการตรวจประเมินทุกปี<br>● ช่วงระยะเวลาการตรวจประเมินระบบการให้บริการจำเป็นต้องใช้ข้อมูลการให้บริการครบทั้ง 365 วัน (1 ปีปฏิทิน) หรือไม่ เช่น ในกรณีที่ผู้ได้รับใบอนุญาตได้รับอนุญาตและประกอบกิจการยังไม่ครบ 1 ปี การตรวจประเมินระบบการให้บริการจะจำกัดเฉพาะช่วงเวลาที่ให้บริการเท่านั้นหรือไม่<br>● ควรปรับเป็น การปฏิบัติตามหลักเกณฑ์การตามลักษณะและมาตรฐานของการให้บริการ<br>● ข้อ 1.4 ควรระบุให้ชัดเจนและครอบคลุมตั้งแต่ต้นปี หากแจ้งภายหลังจะทำให้เป็นภาระในการจัดทำการประเมิน อาจส่งผลให้ไม่สามารถส่งผลประเมินได้ทันตามระยะเวลาที่กำหนด |
| ข้อ 2 ขอบเขตในการตรวจประเมินต้องครอบคลุมระบบการให้บริการสำหรับบริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน บริการยืนยันตัวตน และบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งประกอบด้วยการปฏิบัติงาน กระบวนการทำงาน และระบบงานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง | ● ขอบเขตในการตรวจประเมินควรเป็นการประเมินให้ครอบคลุมตามประเภทบริการ IdP ที่ขออนุญาต เช่น บริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และบริการยืนยันตัวตน ไม่จำเป็นต้องครอบคลุมบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล |
| ข้อ 3 ผู้รับใบอนุญาตต้องดำเนินการประเมินความเสี่ยงให้สอดคล้องตามแนวทางการบริหารจัดการความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของสำนักงานตามรูปแบบที่สำนักงานกำหนด พร้อมจัดส่งผลการประเมินต่อสำนักงานภายใน 30 วันนับแต่วันสิ้นปีปฏิทิน โดยผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมายรับรองผลการประเมินก่อนนำส่งต่อสำนักงาน | ● ขอขยายเป็นส่งผลประเมินภายใน 60 วัน นับแต่วันสิ้นปีปฏิทิน เพื่อมิให้กระบวนการเร่งรัดจนเกินไป<br>● เสนอให้ขยับการส่งรายงานผลการประเมินความเสี่ยงประจำปีเป็นภายใน 31 มีนาคมของปีถัดไป เนื่องจากจะต้องใช้เวลาในการรวบรวมข้อมูล ณ วันสิ้นปีปฏิทิน และจะต้องมีการรายงานให้ผู้บริหาร คณะกรรมการที่ได้รับมอบหมายรับรองก่อนนำส่งให้สำนักงาน รวมถึงจะได้สอดคล้องกับการจัดส่งรายงาน |

| ร่างหลักเกณฑ์ฉบับร่างรับฟังความคิดเห็น | ความคิดเห็น/ข้อเสนอแนะ |
|---|---|
| | ผลการประเมินความเสี่ยงของหน่วยงานกำกับดูแลอื่น เช่น สำนักงาน กลต. ที่จะกำหนดให้ส่งภายในไตรมาส 1 ของทุกปีปฏิทิน<br>● การส่งผลการประเมินภายในระยะเวลา 30 วันนับแต่วันสิ้นปีปฏิทิน อาจทำให้การประเมินมีระยะเวลาที่ค่อนข้างจำกัด ซึ่งอาจส่งผลกระทบ ดังต่อไปนี้<br>1) ผู้รับใบอนุญาต อาจไม่สามารถส่งผลการประเมินได้ทันตามระยะเวลาที่กำหนด เนื่องจากต้องมีการเตรียมการเพื่อเสนอให้ผู้บริหารระดับสูง/คณะกรรมการบริษัทพิจารณาเพื่อรับรองผลการประเมินก่อนนำส่งให้สำนักงาน<br>2) ข้อมูลที่นำมาประกอบการประเมินประจำปีอาจไม่สามารถนำมาประเมินได้ครบทั้ง 365 วัน เช่น อาจขาดข้อมูลในเดือนธันวาคม<br>3) ผู้รับใบอนุญาตในช่วงครึ่งปีหลังของปี อาจมีข้อจำกัดในการเตรียมข้อมูลและการประเมินให้ทัน และครบถ้วน ภายใน 30 วันนับแต่วันสิ้นปีปฏิทิน<br>● มีข้อเสนอแนะ ดังนี้<br>- ขอเสนอเพื่อให้สำนักงานพิจารณาขยายระยะเวลาเป็น 120 วัน นับจากวันสิ้นปีปฏิทิน<br>- ขอเสนอเพื่อให้สำนักงานพิจารณาเพิ่มข้อยกเว้นสำหรับผู้ที่ได้รับใบอนุญาตในช่วงครึ่งปีหลัง ให้สามารถนำส่งรายงานผลการประเมินรวมกับการประเมินในปีถัดไป<br>- หรือเปลี่ยนระยะเวลาการจัดส่งผลการประเมินเป็นภายใน 120 วันนับจากวันครบรอบ 1 ปีที่ได้รับใบอนุญาต<br>● อาจมีการขยายเวลาด้วย เนื่องจากบริษัทอาจมีวันหยุด และภาระงานมากช่วงเดือนมกราคม<br>● ระวังการประเมินความเสี่ยงอาจเข้าข้างตัวเอง |

| ร่างหลักเกณฑ์ฉบับร่างรับฟังความคิดเห็น | ความคิดเห็น/ข้อเสนอแนะ |
|---|---|
| ข้อ 4 การตรวจประเมินตามข้อ 1.4 ต้องกำหนดแผนงานและดำเนินการตรวจประเมินการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง ให้ครอบคลุมส่วนที่มีการเปลี่ยนแปลงของระบบการให้บริการ | - ไม่มีความเห็นเพิ่มเติม - |
| ข้อ 5 การตรวจประเมินตามข้อ 1.1 1.2 และ 1.3 ต้องกำหนดแผนงานและดำเนินการตรวจประเมินให้สอดคล้องกับระดับความเสี่ยงการประกอบธุรกิจของผู้รับใบอนุญาต โดยมีรายละเอียด ดังนี้<br>5.1 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ต้องกำหนดแผนงานและดำเนินการตรวจประเมินการปฏิบัติตามข้อกำหนดให้ครอบคลุมข้อกำหนดทั้งหมดภายใต้หลักเกณฑ์ (full scope) แบบปีเว้นปี<br>5.1.1 ปีที่เป็นการตรวจประเมินให้ครอบคลุมทั้งหมด (full scope) ต้องจัดทำแผนงานและดำเนินการตรวจประเมินให้ครบทุกข้อกำหนดภายใต้หลักเกณฑ์<br>5.1.2 ปีที่ไม่ได้มีการตรวจประเมินให้ครอบคลุมทั้งหมด (full scope) สามารถจัดทำแผนงานและดำเนินการตรวจประเมินข้อกำหนดบางส่วน โดยพิจารณาตามความเสี่ยงและความเหมาะสม<br>5.2 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลางหรือสูง ต้องจัดทำแผนงานและดำเนินการตรวจประเมินการปฏิบัติตามข้อกำหนดให้ครบทุกข้อกำหนดภายใต้หลักเกณฑ์ (full scope) ทุกปี | ● ควรประเมินแบบปีเว้นปี เพราะหากมีการเปลี่ยนแปลงไปจากเดิม ผู้รับใบอนุญาตจะต้องแจ้งสำนักงานเป็นลายลักษณ์อักษรอยู่แล้ว<br>● การตรวจประเมินประจำปี<br>- RLA ต่ำ - ควรตรวจปีเว้นปี<br>- RLA ปานกลาง - ควรตรวจ Full scope ปีเว้นปี แต่ปีที่ไม่ได้ตรวจ Full scope สามารถจัดทำแผนงานและดำเนินการตรวจประเมินข้อกำหนดบางส่วน<br>● ในกรณีที่ผู้รับใบอนุญาตมีผลกระทบความเสี่ยงต่ำในเรื่องนั้น ๆ เช่น การทุจริต หรือการฉ้อโกงจากการใช้งานระบบ อาจมีการประเมินเป็นค่า 0 ในทุก ๆ ปี ในปีถัดไปควรมีการยกเว้นในเรื่องที่เป็นความเสี่ยงต่ำหรือไม่ แล้วก็ค่อยเป็นการส่ง Full scope ในปีถัดไป<br>● อธิบายรายละเอียดของผู้ประกอบธุรกิจที่มีความเสี่ยงปานกลางหรือสูง มีความแตกต่างกันอย่างไร หรือจะมีออกประกาศในอนาคตหรือไม่ แล้วความเสี่ยงในระดับปานกลาง มีหลักเกณฑ์หรือเกณฑ์การประเมินที่แตกต่างกันกับระดับสูงหรือไม่ ควรอธิบายรายละเอียดเพิ่มเติม<br>● ควรลงรายละเอียด หัวข้อขั้นต่ำที่ควรตรวจประเมิน กรณีความเสี่ยงต่ำ |
| ข้อ 6 ผู้รับใบอนุญาตต้องจัดให้มีการตรวจประเมินระบบการให้บริการและรายงานผลการตรวจประเมินระบบ การให้บริการให้สอดคล้องกับหลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ หมวด 3 การตรวจประเมินระบบการให้บริการ | - ไม่มีความเห็นเพิ่มเติม - |

| ร่างหลักเกณฑ์ฉบับร่างรับฟังความคิดเห็น | ความคิดเห็น/ข้อเสนอแนะ |
|---|---|
| ข้อ 7 ผู้รับใบอนุญาตต้องรายงานผลการตรวจประเมินประจำปีตามรูปแบบที่สำนักงานกำหนด ภายใน 30 วัน นับแต่วันที่ดำเนินการตามแผนงานแล้วเสร็จ แต่ไม่เกินวันที่ 31 มกราคมของปีถัดไป | • เสนอให้นำส่งภายใน 60 วัน นับแต่วันที่ดำเนินการตามแผนงานแล้วเสร็จ<br>• เสนอให้ขยับการส่งรายงานผลการตรวจประเมินประจำปีเป็นภายใน 31 มีนาคมของปีถัดไป เนื่องจากจะต้องมีการรายงานให้คณะกรรมการตรวจสอบรับรองก่อนนำส่งให้สำนักงาน รวมถึงจะได้สอดคล้องกับการจัดส่งรายงานผลการตรวจสอบทางด้าน IT ของหน่วยงานกำกับดูแลอื่น เช่น สำนักงาน กลต. ที่จะกำหนดให้ส่งภายใน 3 เดือนนับจากวันสิ้นปีปฏิทินของปีที่เริ่มตรวจสอบ ทั้งนี้ ควรมีเงื่อนไขในการส่งรายงานผลเป็นรอบเวลาเป็นเงื่อนไขเดียวเพื่อให้เข้าใจได้ง่ายในการปฏิบัติ (เดิมเกณฑ์ของสำนักงาน กลต. ก็มีการกำหนดเงื่อนไขไว้ 3 แบบ แต่ก็ได้มีการปรับปรุงให้เป็นรอบเวลาเพียงอย่างเดียว)<br>• การส่งผลการประเมินภายในระยะเวลา 30 วันนับแต่วันสิ้นปีปฏิทิน อาจทำให้การประเมินมีระยะเวลาที่ค่อนข้างจำกัด ซึ่งอาจส่งผลกระทบ ดังต่อไปนี้<br>1) ผู้รับใบอนุญาต อาจไม่สามารถส่งผลการประเมินได้ทันตามระยะเวลาที่กำหนด เนื่องจากต้องมีการเตรียมการเพื่อเสนอให้ผู้บริหารระดับสูง/คณะกรรมการบริษัทพิจารณาเพื่อรับรองผลการประเมินก่อนนำส่งให้สำนักงาน<br>2) ข้อมูลที่นำมาประกอบการประเมินประจำปีอาจไม่สามารถนำมาประเมินได้ครบทั้ง 365 วัน เช่น อาจขาดข้อมูลในเดือนธันวาคม<br>3) ผู้รับใบอนุญาตในช่วงครึ่งปีหลังของปี อาจมีข้อจำกัดในการเตรียมข้อมูลและการประเมินให้ทัน และครบถ้วน ภายใน 30 วันนับแต่วันสิ้นปีปฏิทิน<br>• มีข้อเสนอแนะ ดังนี้<br>- ขอเสนอเพื่อให้สำนักงานพิจารณาขยายระยะเวลาเป็น 120 วัน นับจากวันสิ้นปีปฏิทิน<br>- ขอเสนอเพื่อให้สำนักงานพิจารณาเพิ่มข้อยกเว้นสำหรับผู้ที่ได้รับใบอนุญาตในช่วงครึ่งปีหลัง ให้สามารถนำส่งรายงานผลการประเมินรวมกับการประเมินในปีถัดไป |

| ร่างหลักเกณฑ์ฉบับร่างรับฟังความคิดเห็น | ความคิดเห็น/ข้อเสนอแนะ |
|---|---|
| | - หรือเปลี่ยนระยะเวลาการจัดส่งผลการประเมินเป็นภายใน 120 วัน นับจากวันครบรอบ 1 ปีที่ได้รับใบอนุญาต<br>● สำหรับปี 2568 ควรมีการกำหนดหลักเกณฑ์ให้ชัดเจนก่อน 3-6 เดือน ก่อนให้นำส่งผลการตรวจประเมิน<br>● ควรมีการขอขยายเวลานำส่ง<br>● อาจยืดหยุ่นจนสิ้นเดือนมีนาคมของปีถัดไป |
| ข้อ 8 การรายงานผลการตรวจประเมินประจำปีต่อสำนักงาน ผู้รับใบอนุญาตสามารถรวบรวมผลจากหลายรอบการตรวจประเมินที่ดำเนินการภายในปีปฏิทินเดียวกัน โดยต้องจัดทำรายงานผลการตรวจประเมินประจำปีให้มีรายละเอียดครบถ้วนตามหลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ หมวด 3 การตรวจประเมินระบบการให้บริการ และต้องจัดทำตารางเพื่อแสดงข้อกำหนดภายใต้หลักเกณฑ์และขอบเขตที่ตรวจประเมินในแต่ละรอบการตรวจ เพื่อให้มั่นว่าการตรวจประเมินในแต่ละปีครอบคลุมหลักเกณฑ์และระบบการให้บริการที่เกี่ยวข้อง | ● ในข้อนี้หมายถึงการตรวจของปี 2567 นำรวมส่งในปี 2568 ใช่หรือไม่ แล้วต้องนำส่งในรอบเดือนใด ควรกำหนดเป็นหลักเกณฑ์ให้ชัดเจนเพื่อไม่ให้เกิดความสับสน และได้สะดวกต่อการดำเนินการตามแผนงานที่กำหนด |
| ข้อ 9 ผู้รับใบอนุญาตต้องจัดเก็บรายงานผลการตรวจประเมินไว้เป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำรายงาน เพื่อให้พร้อมสำหรับการตรวจสอบหรือเมื่อร้องขอโดยสำนักงาน | ● รูปแบบการจัดเก็บผลควรสามารถจัดเก็บในลักษณะไฟล์ หรือระบบอิเล็กทรอนิกส์ได้ เพื่อสะดวกแก่การเรียกตรวจ<br>● เสนอให้กำหนดว่าเก็บเฉพาะรายงานผลการตรวจ หรือหลักฐานที่ใช้ประกอบการตรวจเนื่องจากการจ้าง External Audit จะได้เฉพาะรายงานเท่านั้น หากจำเป็นต้องมีเอกสารจะได้สามารถระบุในการจ้างได้ |
| **ส่วนที่ 2 การพิจารณาความมีนัยสำคัญ** | |
| ข้อ 10 ผู้รับใบอนุญาตต้องจัดให้มีข้อกำหนดในการพิจารณาความมีนัยสำคัญหรือความสำคัญที่ชัดเจนเพื่อใช้พิจารณาดำเนินการในเรื่องต่าง ๆ โดยดำเนินการดังนี้ | ● เสนอให้ทบทวนเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ<br>● ข้อกำหนดนี้ ไม่เกี่ยวกับการตรวจประเมินประจำปี ควรพิจารณาทำเป็นหลักเกณฑ์แยก หรือข้อชี้แจงเพิ่มเติมออกมาเพื่อขยายความหลักเกณฑ์ต่าง ๆ ใน ธพส. 1/2566 ที่เกี่ยวข้อง |

| ร่างหลักเกณฑ์ฉบับร่างรับฟังความคิดเห็น | ความคิดเห็น/ข้อเสนอแนะ |
|---|---|
| 10.1 ข้อกำหนดดังกล่าวต้องผ่านการพิจารณาร่วมกันของหน่วยงานที่เกี่ยวข้อง รวมทั้งต้องได้รับอนุมัติจากผู้บริหาร คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมาย<br>10.2 ข้อกำหนดในการพิจารณาความมีนัยสำคัญต้องพิจารณาภายใต้กรอบหลักการที่คำนึงถึง<br>ความเสี่ยงและผลกระทบต่อการให้บริการของผู้รับใบอนุญาตในวงกว้าง เช่น กระทบลูกค้าหรือผู้ใช้บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของผู้รับใบอนุญาต และคำนึงถึงผลกระทบต่อระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลใน<br>วงกว้าง เช่น กระทบต่อระบบงานกลางที่มีนัยสำคัญเชิงโครงสร้างต่อการให้บริการของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล<br>10.3 ต้องทบทวนข้อกำหนดอย่างน้อยปีละ<br>1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าข้อกำหนดดังกล่าวสอดคล้องกับ<br>ระดับความเสี่ยงและผลกระทบต่อการให้บริการ | ● ขอให้คำชี้แจงเพิ่มเติมเกี่ยวกับกำหนดเวลาที่ต้องทบทวนข้อกำหนดในการพิจารณาความมีนัยสำคัญ ต้องจัดทำในรอบการทบทวนผลการประเมินต่อสำนักงานภายในประจำปีหรือไม่ หรือสามารถดำเนินการเมื่อบริษัทฯ เห็นสมควรได้ภายในรอบทบทวน 1 ปี<br>● ในประเด็นนี้ผู้รับใบอนุญาต จะต้องมีการกำหนด Policy ใช่หรือไม่ และควรมีการกำหนดหลักเกณฑ์และเรื่องอะไรบ้างที่มีความสำคัญ ต้องมีความแตกต่างจากเกณฑ์การประเมิน หรือมีการพิจารณาตามบริบทของผู้ขอรับใบอนุญาตในกรณีไหนบ้าง หากเป็น สูง กลาง ต่ำ ต้องประเมินอย่างไร มีการประเมินในกลุ่มใดบ้าง ควรมีการกำหนดให้ชัดเจน<br>● หากเป็นกรณีที่ผู้รับใบอนุญาตฯ ได้รับการประเมิน ISO 27001 แล้ว และได้มีการประเมินบริบทขององค์กรผ่านการประเมิน Internal Context และ External Context ที่มีขอบเขตตั้งแต่ Interested Party ไปจนถึงผู้ใช้บริการ (user) สามารถใช้เอกสารตัวนี้ทดแทนกันได้หรือไม่ |
| ข้อ 11 ผู้รับใบอนุญาตต้องสื่อสารข้อกำหนดดังกล่าวให้แก่บุคลากรและบุคคลภายนอกที่เกี่ยวข้องทราบและนำไปปฏิบัติ | ● ข้อกำหนดนี้ ไม่เกี่ยวกับการตรวจประเมินประจำปี ควรพิจารณาทำเป็นหลักเกณฑ์แยก หรือข้อชี้แจงเพิ่มเติมออกมาเพื่อขยายความหลักเกณฑ์ต่าง ๆ ใน ธพส. 1/2566 ที่เกี่ยวข้อง |
| **ส่วนที่ 3 การแจ้งการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่ส่งผลกระทบต่อการให้บริการ** | |
| ข้อ 12 การแจ้งนำเทคโนโลยีมาใช้ หรือการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่ส่งผลกระทบต่อการให้บริการ<br>12.1 ผู้รับใบอนุญาตที่นำเทคโนโลยีมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยี โดยการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าวมีนัยสำคัญตามข้อกำหนดที่ผู้รับใบอนุญาตได้กำหนดขึ้นตามข้อ 10 ทั้งกรณีที่ผู้รับใบอนุญาตดำเนินการเองและกรณีที่มีการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก | ● ข้อกำหนดนี้ ไม่เกี่ยวกับการตรวจประเมินประจำปี ควรพิจารณาทำเป็นหลักเกณฑ์แยก หรือข้อชี้แจงเพิ่มเติมออกมาเพื่อขยายความหลักเกณฑ์ต่าง ๆ ใน ธพส. 1/2566 ที่เกี่ยวข้อง โดยหลักเกณฑ์ที่เกี่ยวข้อง ซึ่งควรนำหลักการพิจารณานัยสำคัญมาใช้ ตัวอย่างเช่น<br>- แนบท้ายประกาศ สพธอ. ที่ธพส. 1/2566 ฉบับที่ 5 หลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการ ข้อ 25 กรณีที่มีการเปลี่ยนแปลงระบบหรือ |

| ร่างหลักเกณฑ์ฉบับร่างรับฟังความคิดเห็น | ความคิดเห็น/ข้อเสนอแนะ |
|---|---|
| ต้องแจ้งการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าวต่อสำนักงานล่วงหน้าไม่น้อยกว่า 30 วันก่อนดำเนินการ ตามรูปแบบและวิธีที่สำนักงานกำหนด เว้นแต่สำนักงานมีคำสั่งให้ผู้รับใบอนุญาตไม่ต้องแจ้งการนำเทคโนโลยีมาใช้ หรือเปลี่ยนแปลงระบบหรือเทคโนโลยีที่มีนัยสำคัญ | เทคโนโลยีที่ส่งผลกระทบต่อระบบการให้บริการภายหลังจากเริ่มประกอบธุรกิจผู้รับใบอนุญาตต้องดำเนินการตรวจประเมินระบบในส่วนที่ได้รับผลกระทบจากการเปลี่ยนแปลงดังกล่าวและนำส่งรายงานผลการตรวจประเมินพร้อมการแจ้งการเปลี่ยนแปลงต่อสำนักงาน<br>- แนบท้ายประกาศ สพธอ. ที่ธพส. 1/2566 ฉบับที่ 3 หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ ข้อ 22 กรณีที่มีการเปลี่ยนแปลงระบบหรือเทคโนโลยีที่ส่งผลกระทบต่อระบบการให้บริการภายหลังจากเริ่มประกอบธุรกิจผู้รับใบอนุญาตต้องจัดให้มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลและนำส่งผลการประเมินพร้อมการแจ้งการเปลี่ยนแปลงต่อสำนักงาน<br>● ขอให้ยกตัวอย่าง Use Case การเปลี่ยนแปลงระบบ หรือเทคโนโลยีที่มีนัยสำคัญ ที่ต้องแจ้งไปยังสำนักงานล่วงหน้าไม่น้อยกว่า 30 วัน<br>● เมื่อมีการแจ้งการนำเทคโนโลยีมาใช้งานแล้ว ควรจะต้องมีการรอรับผลการแจ้งหรือการพิจารณาด้วยหรือไม่ ว่าใช้ได้หรือไม่ได้ ควรกำหนดให้ชัดเจน<br>● ควรมีการกำหนดรูปแบบมาตรฐานการเชื่อมต่อ และแยกหมวดประเภทการเชื่อมต่อให้ชัดเจน ยกตัวอย่างเช่น<br>- การเชื่อมต่อกับ RP เป็นการเชื่อมต่อแบบมาตรฐานไม่ต้องแจ้ง<br>- การเชื่อมต่อกับ IDP จะต้องแจ้ง<br>- การเปลี่ยนระบบกรณีฉุกเฉิน (Incident) ควรแจ้งได้ภายหลัง |

**ความเหมาะสมของแนวทางการประเมินระดับความเสี่ยงขององค์กร**

| ร่างหลักเกณฑ์ฉบับร่างรับฟังความคิดเห็น | ความคิดเห็น/ข้อเสนอแนะ |
|---|---|
| คำถามสำหรับการประเมินความเสี่ยงมีความชัดเจน เหมาะสม และครอบคลุมความเสี่ยงจากการให้บริการ DID หรือไม่ | ● ข้อ 63 ควรกำหนดขอบเขตจำนวนผู้อาศัยการยืนยันตัวตน (RP) ให้ชัดเจน โดยให้หมายถึง RP ที่เรียกใช้บริการของธนาคารในปีนั้น ๆ เท่านั้น เนื่องจากธนาคารจะไม่ทราบข้อมูลจำนวน RP ทั้งหมดในระบบ<br>● ควรมีคำอธิบายว่า สูง กลาง และต่ำ มีความแตกต่างกันอย่างไรในเรื่องการประเมินความเสี่ยงนั้น ๆ |
| เกณฑ์ที่นำมาใช้ประเมินความเสี่ยงในแต่ละข้อคำถามมีความเหมาะสมหรือไม่ | ● หลักเกณฑ์ที่กำหนดในข้อ 65 ข้อ 69 และข้อ 70 นั้น ควรนำปริมาณธุรกรรมที่เกิดขึ้นจริงในระบบ มาใช้ประกอบการกำหนดความห่างที่เหมาะสม เนื่องจากหลักเกณฑ์ที่กำหนดในปัจจุบัน อาจทำให้ผู้ได้รับอนุญาตทั้งหมดตกอยู่ในความเสี่ยงระดับสูง และไม่สามารถแยกระดับความเสี่ยงที่แท้จริงได้<br>● จากส่วนการคิด "ปัจจัยเสี่ยง : ด้านประวัติเหตุการณ์ไม่พึงประสงค์" ควรคิดแบบฐานนิยม หรือค่าเฉลี่ย<br>● จาก ข้อ 18 จำนวนเหตุการณ์การทุจริตหรือการฉ้อโกงจากการใช้งานระบบการให้บริการ Digital ID ในรอบปีปฏิทินล่าสุด เช่น การถูกปลอมแปลงตัวตน<br>- ควรปรับค่า Criteria ระดับความเสี่ยงต่ำ /ปานกลาง/สูง เช่น<br>○ สูง ต้องไม่เกินค่า FAR > 0.1% (อ้างอิงตามระดับ FAR ของ ธปท.)<br>○ ปานกลาง และต่ำ ควรลดหลั่นกันตามความเหมาะสม<br>● จากข้อ 59 จำนวนการใช้บริการจากผู้รับดำเนินการแทนในการให้บริการ<br>- ควรปรับค่า Criteria ของระดับความเสี่ยงต่ำ ให้มีจำนวนผู้รับดำเนินการแทน ส่วนระดับความเสี่ยงปานกลาง และสูงก็เพิ่มขึ้นตามความเหมาะสม เนื่องจากในธุรกิจปัจจุบันจำเป็นต้องมีผู้รับดำเนินการแทนเพื่ออำนวยความสะดวกแก่ลูกค้า<br>● ประเด็นใน Part 4 เรื่องกรณีเป็นบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัลนั้น หากจำนวนยอด Transaction ต่อปี |

| ร่างหลักเกณฑ์ฉบับร่างรับฟังความคิดเห็น | ความคิดเห็น/ข้อเสนอแนะ |
|---|---|
| | มี Transaction สูง ทำไมระดับความเสี่ยงจึงไปตกที่สูง ทั้งที่การให้บริการก็อยู่บนระบบการให้บริการแบบเดิมและเทคโนโลยีเดิมไม่ได้เปลี่ยนแปลงไป |
| ข้อเสนอแนะอื่น ๆ เพิ่มเติม | • หลักเกณฑ์นี้ครอบคลุมเฉพาะการตรวจประเมินประจำปี แต่ในประกาศ ธพส. 1/2566 ยังกำหนดให้มีการรายงานประจำปีในหลายเรื่องด้วย ขอให้สำนักงานพิจารณาเรื่องที่มีความเกี่ยวข้องกันเพื่อลดความซ้ำซ้อนในการปฏิบัติ<br>• เสนอให้ สพธอ. พิจารณาให้ผู้ได้รับใบอนุญาตประกอบธุรกิจ ได้รับยกเว้นการตรวจประจำปีในปีแรกของการปฏิบัติงาน เนื่องจากได้ทำการตรวจสอบความพร้อมของระบบการใช้งานเรียบร้อยแล้ว<br>• สอบถามอัตราค่าธรรมเนียม ผู้ประกอบธุรกิจยังจะต้องเสียในอัตราเท่าไหร่<br>• ควรมีการจัด review หลักเกณฑ์ และประชาสัมพันธ์ให้ผู้รับใบอนุญาติประจำปี<br>• อยากให้ สพธอ. คุยกับ ธปท. แล้วพัฒนา แนวการประเมินร่วมกัน และใช้รายงานฉบับเดียวกัน<br>• ควรจัดทำคู่มือและข้อกำหนดสำหรับการตรวจประเมินเพื่อจัดทำแผนการตรวจและนำหลักฐานการตรวจมาสนับสนุนให้ชัดเจน เพื่อความสอดคล้องกับมาตรฐานอื่น ๆ ภายในองค์กร |

**รายชื่อบริษัทที่ร่วมแสดงความคิดเห็น**

1. บริษัท ทรู มูฟ เอช ยูนิเวอร์แซล คอมมิวนิเคชั่น จำกัด
2. ธนาคารเกียรตินาคินภัทร จำกัด (มหาชน)
3. ธนาคารกสิกรไทย จำกัด (มหาชน)
4. บริษัท ช้อปปี้เพย์ (ประเทศไทย) จำกัด
5. บริษัท เนชั่นแนลดิจิทัลไอดี จำกัด
6. บริษัท ไทยไอเด็นติตี้ส์ จำกัด
7. ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร
8. ธนาคารไทยเครดิต จำกัด (มหาชน)
9. บริษัท ดาต้าวัน เอเชีย (ประเทศไทย) จำกัด
10. ตลาดหลักทรัพย์แห่งประเทศไทย
11. บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
12. บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)